



PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G08B 13/14	A1	(11) International Publication Number: WO 98/25243 (43) International Publication Date: 11 June 1998 (11.06.98)
<p>(21) International Application Number: PCT/GB97/03277</p> <p>(22) International Filing Date: 28 November 1997 (28.11.97)</p> <p>(30) Priority Data: 9624981.8 30 November 1996 (30.11.96) GB</p> <p>(71) Applicant (for all designated States except US): WATKINS, Daryl, Joclyn [GB/GB]; 12/13 The Street, Yatesbury, Calne, Wiltshire SN11 8YG (GB).</p> <p>(71)(72) Applicant and Inventor: WATKINS, Richard [GB/GB]; 12/13 The Street, Yatesbury, Calne, Wiltshire SN11 8YG (GB).</p> <p>(74) Agents: LAINE, Simon, James et al.; Wynne-Jones, Laine James, 22 Rodney Road, Cheltenham, Gloucestershire GL50 1JJ (GB).</p>		<p>(81) Designated States: CN, JP, RU, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Published <i>With international search report.</i></p>
<p>(54) Title: IMPROVEMENTS RELATING TO SECURITY SYSTEMS</p> <div data-bbox="302 1167 1260 1461"> <pre> graph LR 1[Master 1] --- 3[Bus 3] 3 --- 2_1[Slave 2] 3 --- 2_2[Slave 2] 3 --- 2_3[Slave 2] 3 --- 2_4[Slave 2] 3 --- 2_5[Slave 2] 3 --- 2_6[Slave 2] </pre> </div> <p>(57) Abstract</p> <p>A security system, particularly for a computer network, carries out surveillance of slave components (2) from a master (1), conveniently through existing cabling (3). The slaves (2) are interrogated on a cyclic basis and a signal goes back to the master to determine if there is any departure from normality. A supervisor at the master can identify the component and can interrogate in more detail to determine what has happened at that component, for example whether it has been disconnected, moved or partially dismantled, or is being used illicitly. An alarm (9) may be triggered by an abnormal response, and security measures brought into action.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China	KZ	Kazakhstan	PT	Portugal		
CU	Cuba	LC	Saint Lucia	RO	Romania		
CZ	Czech Republic	LI	Liechtenstein	RU	Russian Federation		
DE	Germany	LK	Sri Lanka	SD	Sudan		
DK	Denmark	LR	Liberia	SE	Sweden		
EE	Estonia			SG	Singapore		

"Improvements relating to Security Systems"

This invention relates to security systems. It is particularly concerned with the security of computer installations where the components may be spread around different rooms and different floors in a building. They will of course be interconnected by cables, and one aim is to use where possible the existing cables as part of the security network, without the need to provide further inter-component wiring. It should therefore be fairly non-disruptive to instal such a system.

The system could also be applied to other combinations of electrical/electronic components, for example hi-fi systems with tuners, amplifiers, CD players, turntables, tape recorders and speakers, or TV sets and video recorders. It is also applicable to non-electrical items, such as a set of filing cabinets, although of course dedicated cabling will then have to be provided. But generally reference will be made just to computer systems.

There are various security devices already in use. Some employ tremblers so that when a component is physically disturbed a circuit is closed and an alarm is generated. But this requires power always to be available at that component, and if it is switched off (as it is likely to be at a time when someone is attempting to remove it) then there has to be separate provision, mains or battery, for the alarm device. This is not ideal. Therefore another aim of the present system is to be able to monitor switched-off

components without local, auxiliary powered devices.

Such known devices also have the disadvantage that, if separately powered, they can remain primed while the component is in use, and can therefore be triggered if the user makes an adjustment or simply knocks it accidentally, or shifts his desk for example. This system should avoid such faults.

According to the present invention there is provided a security system for a plurality of components linked by cable, such as a computer system, wherein one component is equipped with a master monitoring device (the master) and the other components are equipped with slave monitoring devices (the slaves) individually identifiable to the master, wherein the master is programmed to interrogate the slaves on a cyclic basis via cable and wherein if there is a response (or lack of response) indicating a departure from normality, the relevant slave is noted by the master.

Conveniently, the interrogation should be by existing cabling linking the components, provided that is non-interfering with other functions. But it may be necessary occasionally to use dedicated cabling for the interrogation.

Conveniently, the interrogation has two modes, the first being the cyclic interrogation of the slaves which will give a basic yes/no indication of normality, and the second being a more detailed interrogation of a slave that produces a no indication. In other words, a basic interrogation may simply indicate that something is wrong with a particular component. For further details, the master goes

into the second interrogation mode, in which it targets this component and determines the fault in more detail. This switch into the second mode will preferably be automatic, although it could be done by the supervisor.

5 The network may be capable of having further components connected. The interrogation can be extended to cover nodes where such connections may be made, whereby the addition of a component to the network is signalled to the master.

10 The master should be re-programmable to note a slave which has an authorised departure from normality, and not to register an alarm while that departure lasts.

15 This is to cater for occasions when unplugging or lid removal is quite in order, as when an office is re-arranged or when servicing is carried out. An unnecessary alarm is suppressed if the master is temporarily re-programmed effectively with the knowledge that a certain component is to be disrupted in a certain way. The interrogation procedure is modified accordingly to ignore the predicted fault signal.

20 The master is conveniently programmable with details of each slave and is equipped with display means enabling a supervisor at the master to review such details at least in the event of that slave departing from normality.

25 In more detail, the supervisor can have a screen on which information relating to the system can be displayed, conveniently in graphic form. In memory can be stored information on each monitored component, such as the name of the normal user, his telephone or extension number, similar

details on any back-up user, the location of the component, its description (printer, for example), possibly with more details such as maker and model number, and any other relevant data. Should attention be brought to that component, the supervisor can then immediately call up this information.

The detectable departures from normality may include a selection of disconnection, physical movement, at least partial dismantling, use, and whether the slave is switched on or off.

The most basic fault to detect is a slave disconnection, as when an electrical/electronic component is unplugged or its cable is cut so that it can be removed. When this happens, there will of course be no "OK" response to the master when that component is interrogated, and so a problem there is identified. While this could be arranged to raise a general external alarm, it might well be preferred quietly to alert the person overseeing the system (the supervisor), and possibly also automatically to bring security cameras to bear, and to lock doors, all with a view to identifying and trapping a thief. The supervisor could choose the type of response required.

Often, it is not the whole component in which a thief is interested; it might be just a chip in a P.C. for example. Access to it requires a lid or backing to be removed, and this can be linked to the slave within the P.C. so that, on interrogation, the message will be passed back to the master that such lid removal has been effected.

Another use could simply be to determine whether a component is switched on or not. While this would not excite remark during normal office hours, it would be interesting outside them. It could simply mean that the component was
5 accidentally left switched on, wasting power, but it could also indicate illicit out-of-hours use, perhaps by someone trying to obtain sensitive information.

The master will continue at each cycle to interrogate the disconnected or otherwise faulty or interfered-with
10 component after the initial alarm is raised. If the unplugged cable is re-connected, or the lid re-fitted, there is affirmative feedback and the alarm may be arranged to stop, although a record of the fault may remain at the master, to be investigated if necessary. If the disconnec-
15 tion or lid removal is repeated, the alarm trips on again. Provision will also generally be made for the supervisor to suppress the alarm, once it has been raised.

It is envisaged that the system could be adapted to monitor combinations of articles or structures other than
20 electrical/electronic components of a portable nature. For example, it could serve a group of buildings, each building being a slave station except for one accommodating the master. Each building would have its own security system reporting in to its slave, and the slaves would be cyclical-
25 ly checked by the master. As well as intruder sensing, there could be smoke and heat sensing, to give early warning to the master of fire.

For a better understanding of the invention, one

embodiment will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a diagram of a simple computer network,

Figure 2 is a block diagram of a security system
5 control card for a master station,

Figure 3 is a more detailed circuit diagram of the master control card, particularly in relation to the microprocessor and memory,

Figure 4 is a more detailed circuit diagram of a
10 network control and interface of the master control card,

Figure 5 is a more detailed circuit diagram of an output control and interface of the master control card,

Figure 6 is a more detailed circuit diagram of a "watchdog" timer of the master control card with an over -
15 current timer not apparent in Figure 3,

Figure 7 is a more detailed circuit diagram of a bus interface of the master control card,

Figure 8 is a block diagram of a security system control card for a slave station,

20 Figure 9 is a more detailed circuit diagram of the slave station card, and

Figure 10 is a flow chart associated with a slave station.

The network of Figure 1 has a master computer 1 and
25 several other computers 2 (the slaves) at various work-stations, all interconnected by cable 3 through which they can communicate. Generally, these computers will be individually powered, so that they can be switched on and

off, or plugged in and unplugged, separately.

In addition to the circuitry and components that make the computers perform their ordinary functions, they will be equipped with circuit boards (or cards for brevity) for the security system, the master 1 having the card 4 of Figure 2 and the slaves each having the card 5 of Figure 8. These slave cards are not reliant on the associated computer being plugged in to a power socket and switched on: each slave card is energised from the master 1 via the cable 3.

10 The master card 4 has a microprocessor 6 with an associated memory 7, the microprocessor communicating with the cable 3 via a network control and interface 8 and operating an alarm system 9 through an output control and interface 10. The alarm system 9 may be both remote and
15 local and include more than simply audible and/or visible indications of abnormality. There could be CCTV cameras to activate, or door closures to lock, for example. The card also has a watchdog circuit 11, to be described later, and is shown with an interface 12 for connecting to a bus 13. In
20 the conventional way, broad arrows indicate multi-channel communication, while the single line arrows represent single channels.

Figure 3 shows this card in more detail. Suitable components and their terminals are identified here and in
25 other figures by code numbers and abbreviations that will be known to those familiar with computer construction. The various connections are also shown in conventional form and so detailed description will not be given.

Further details on circuits 8, 10, 11 and 12 are shown in Figures 4 to 7 respectively. Again, conventions are followed and they will not be described in detail.

The network control and interface circuit 8 of Figure 4 has a power control sub-circuit 14 and network ports 15 with a precautionary over-current sensing circuit 16. A short in a cable would cause a current surge, and this circuit will react immediately to protect the network ports 15, closing them down as necessary.

Figure 6 shows the watchdog timer circuit 11 in conjunction with an over-current timer 17. This is not shown separately in Figure 2, being shared by the microprocessor 6 and the interface 8. The watchdog circuit 11 is provided as a check on the microprocessor 6 and the rest of the main card. Unless neutralised by the microprocessor working normally, it issues a reset signal at regular intervals. In other words it sets the microprocessor going again should it suffer "lock up". Should the sensing circuit 16 have cut in, it will allow time for the system to settle down and then it will allow re-energisation.

Referring now to Figure 8, each slave card 8 has a microprocessor 18, memory 19, address selector 20, network interface 21 and power sensing interface 22. There is also at least one auxiliary port interface 23. The interface 21 connects to the cable 3, and the interface 22 (which is optional) to the bus 13. A lid detector 24 will send a signal directly to the microprocessor 18 should a lid, back panel or other part of the associated computer 2 be removed.

The port interface 23 receives a signal from any connected peripheral 25, such as a printer, that is required to be monitored.

Figure 9 shows the card 8 in more detail, Figures 8 and 5 9 following the conventions and style of Figures 2 and 3.

In operation, switch-on at the master 1 initialises the card 4. Then that sends out its first interrogation to an identifiable node (where usually a computer 2 is connected). A timer is set and the master stays dormant. When data is 10 returned from the first node, it is re-activated and checks whether that data is correct or not. If it is correct, then interrogation of the second node is carried out similarly, and so on. But if there is a return signal signifying something wrong the alarm system 9 will be triggered.

15 If there is no signal back by the end of the timer period, this triggers a check against the memory 7, which might have been programmed to record that there is nothing at the node in question and that a null response is to be expected. In that case, the interrogation of the next node 20 continues as normal. But if a null response is incorrect, the alarm 9 is activated.

At each slave, the interrogation puts in train the events of the flow chart of Figure 10. Each time, the address in the interrogation signal is checked against the 25 home address and if there is no match, the slave card remains dormant. But when the right signal does arrive a set of checks is carried out and a reply sent back to the master.

If the master is unplugged or incapacitated, this will trigger an external alarm. Obviously, there can be no detailed diagnosis of the fault but at least someone should be alerted. Also if the cable between the interface 10 on
5 the card 4 and the alarm system 9 is cut or unplugged, an alarm will be generated by that system.

CLAIMS

1. A security system for a plurality of components linked by cable, such as a computer network, wherein one component is equipped with a master monitoring device (the master) and the other components are equipped with slave monitoring devices (the slaves) individually identifiable to the master, wherein the master is programmed to interrogate the slaves on a cyclic basis via cable, and wherein if there is a response (or lack of response) indicating a departure from normality, the relevant slave is noted by the master.

2. A security system as claimed in Claim 1, wherein the interrogation is via existing cabling linking the components.

3. A security system as claimed in Claim 1 or 2, wherein the interrogation has two modes, the first being the cyclic interrogation of the slaves which will give a basic yes/no indication of normality, and the second being a more detailed interrogation of a slave that produces a no indication.

4. A security system as claimed in Claim 1, 2 or 3, wherein the network is capable of having further components connected, and wherein the interrogation covers nodes where such connections may be made, whereby the addition of a component to the network is signalled to the master.

5. A security system as claimed in any preceding claim, wherein the master is re-programmable to note a slave which has an authorised departure from normality, and not to register an alarm while that departure lasts.

6. A security system as claimed in any preceding claim, wherein the master is programmable with details of each slave and is equipped with display means enabling a supervisor at the master to review such details at least in
5 the event of that slave departing from normality.

7. A security system as claimed in any preceding claim, wherein the detectable departures from normality include a selection of disconnection, physical movement, at least partial dismantling, use, and whether the slave is
10 switched on or off.

1/10

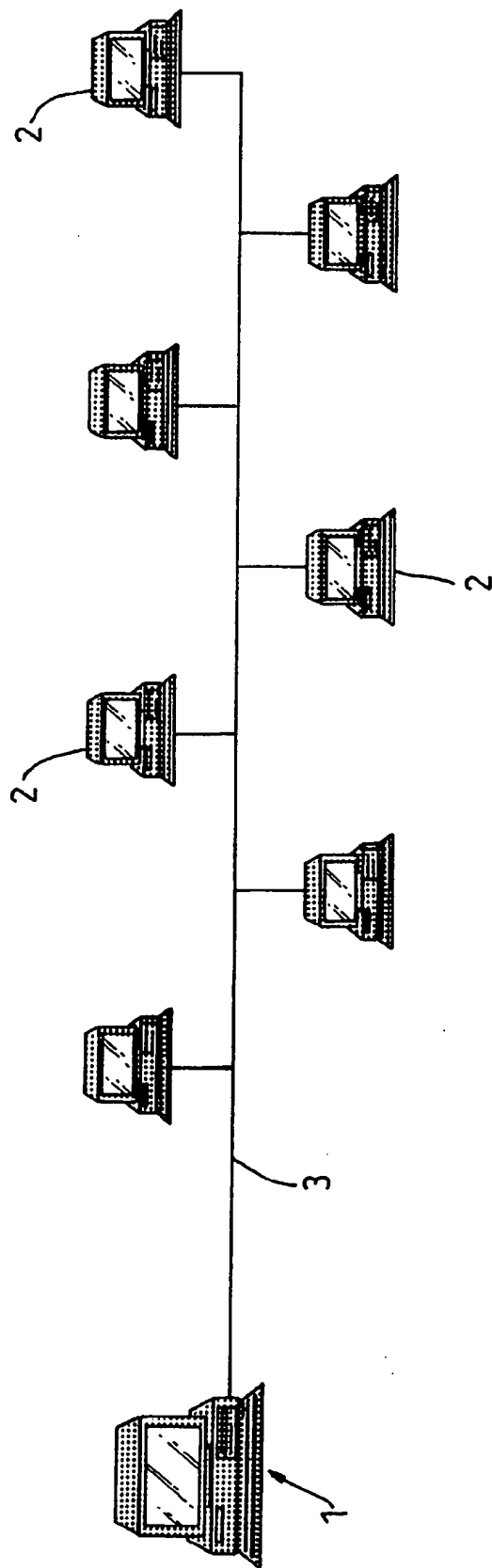


Fig. 1

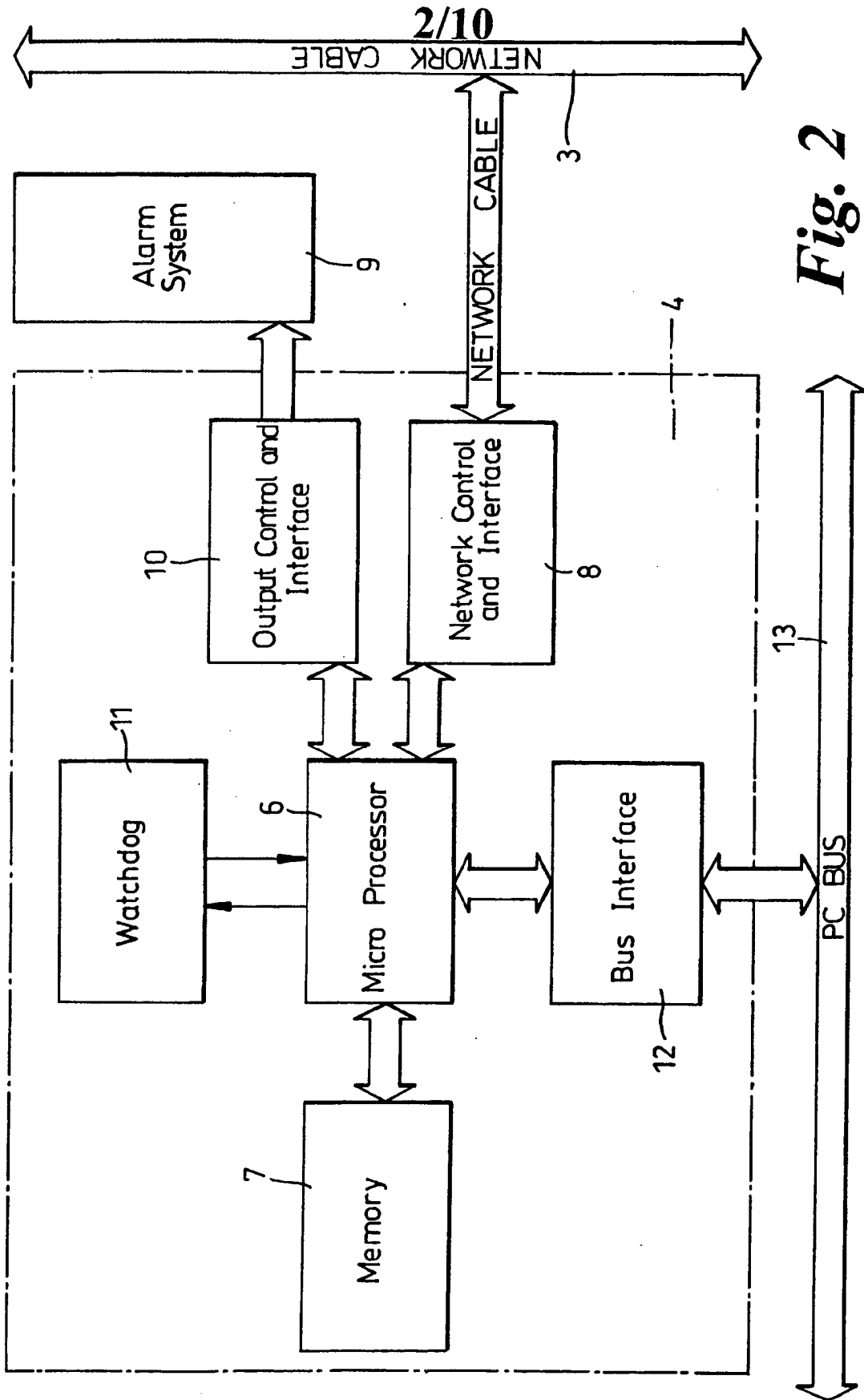


Fig. 2

3/10

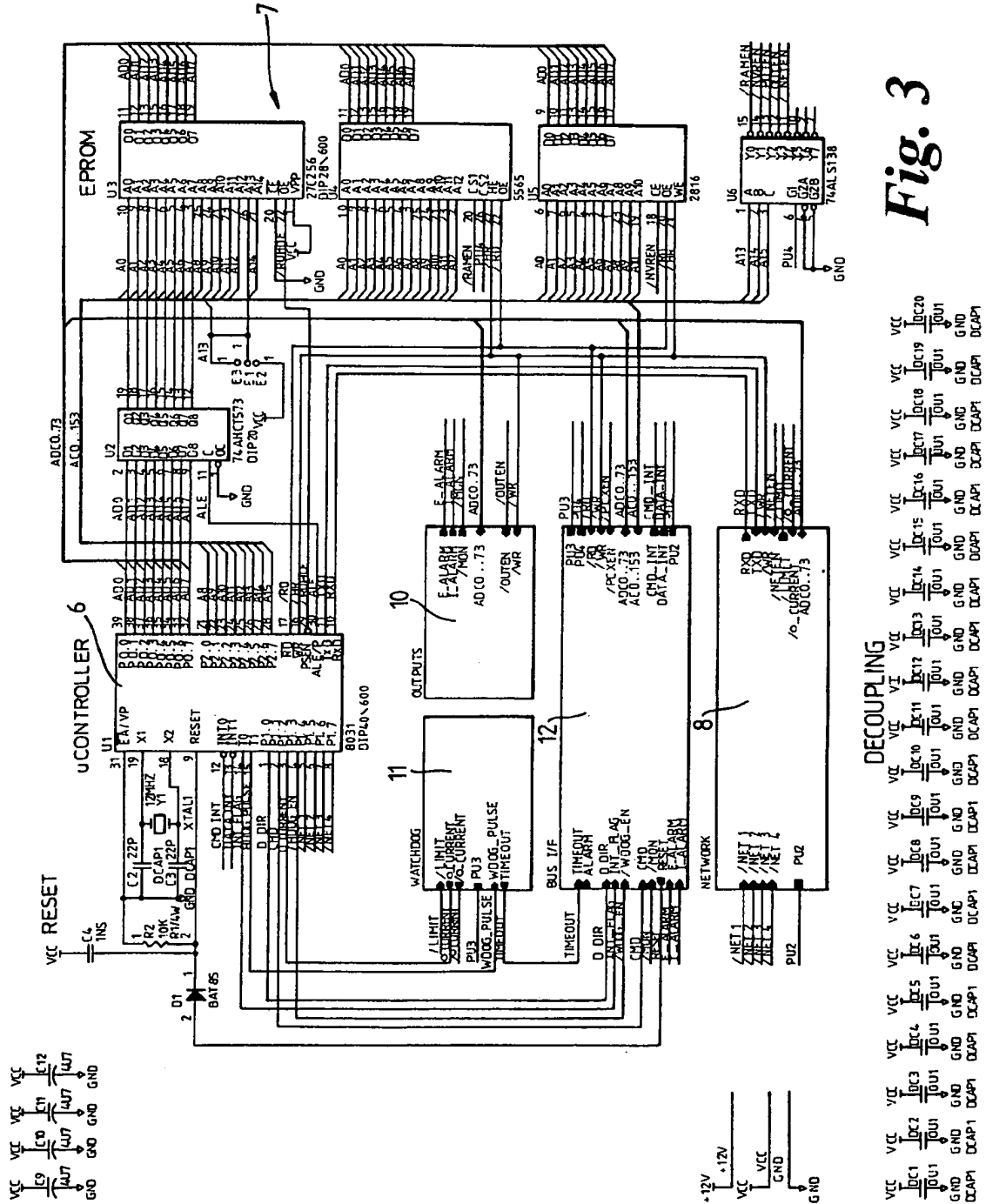


Fig. 3

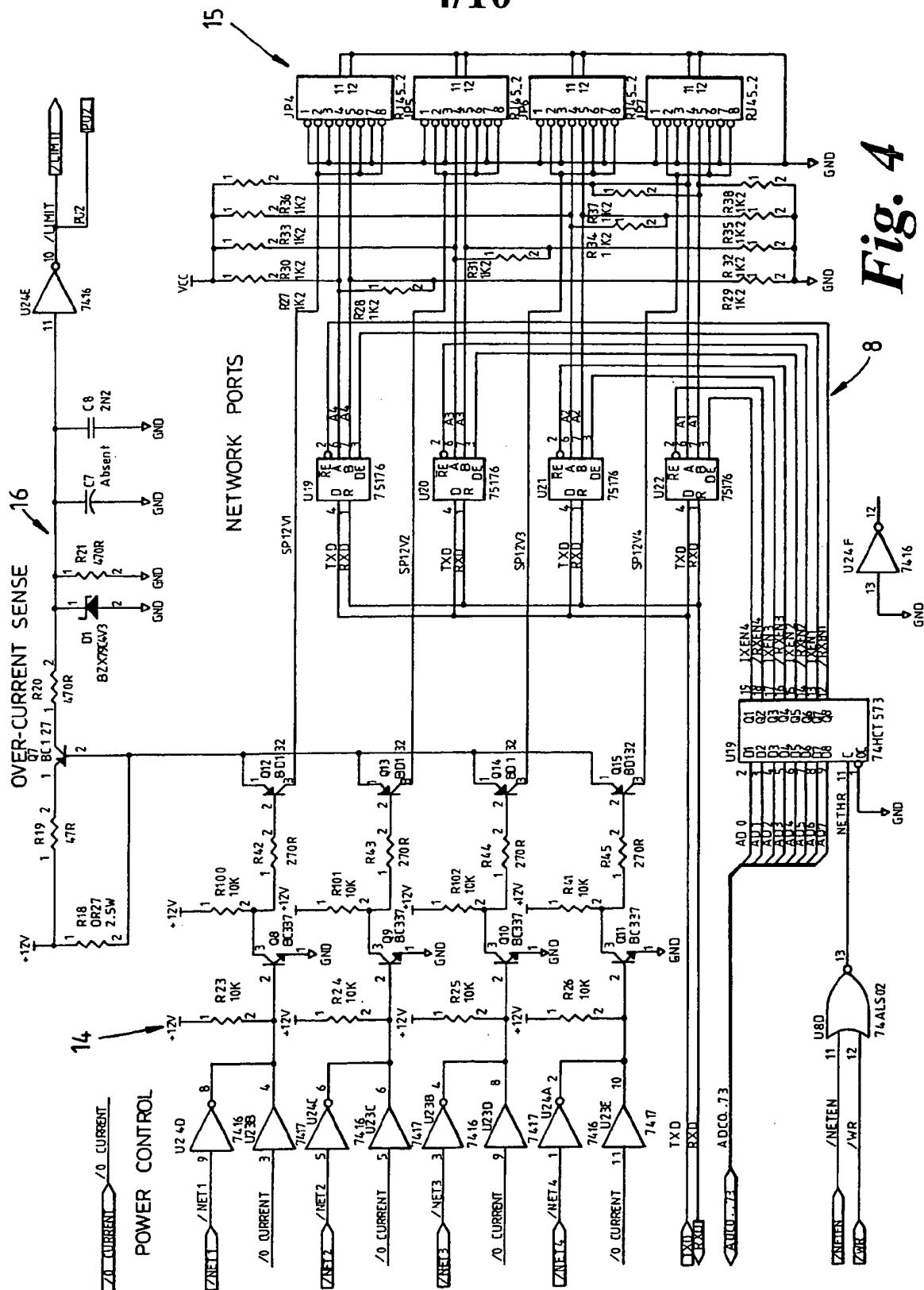


Fig. 4

5/10

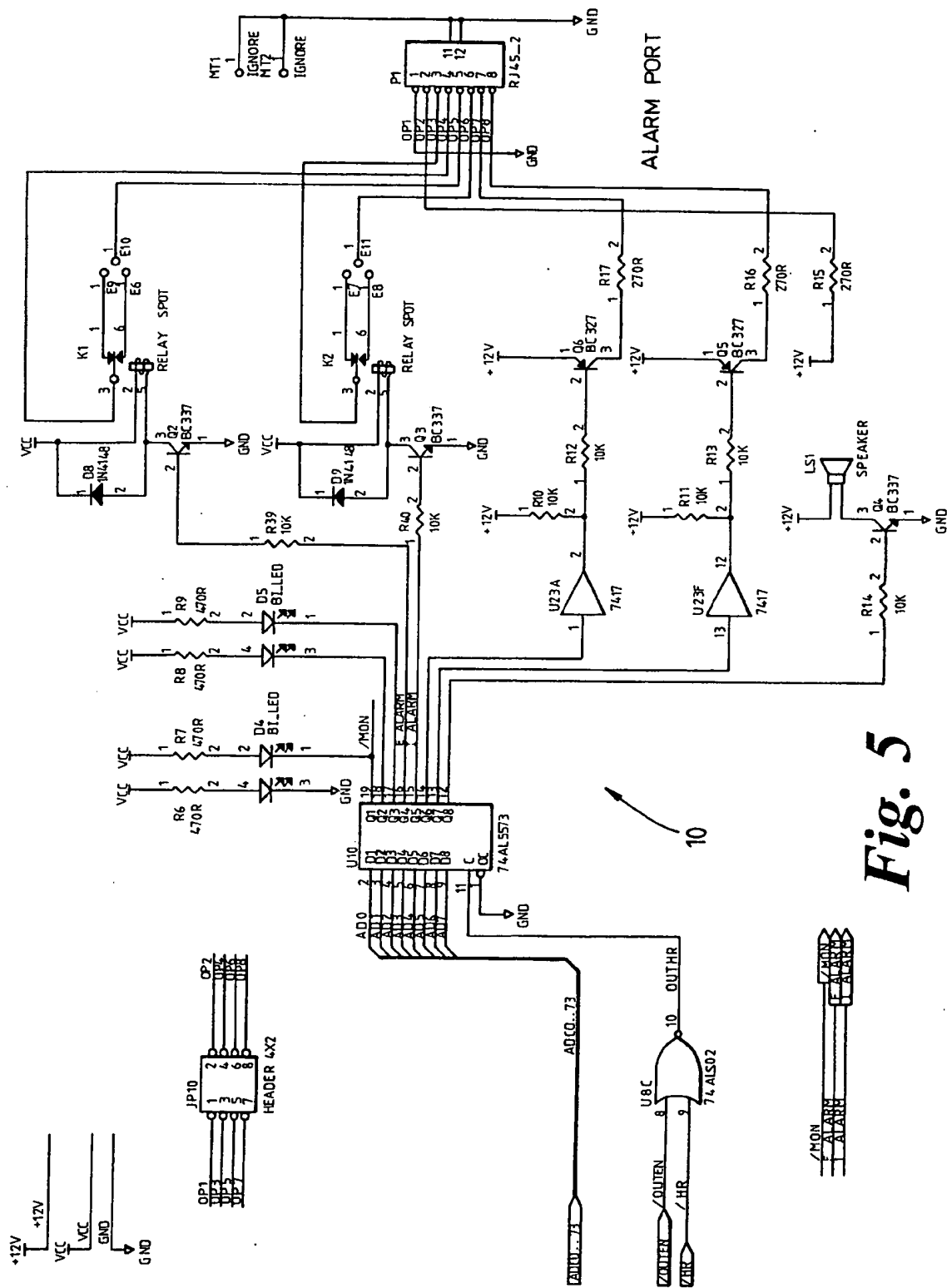


Fig. 5

6/10

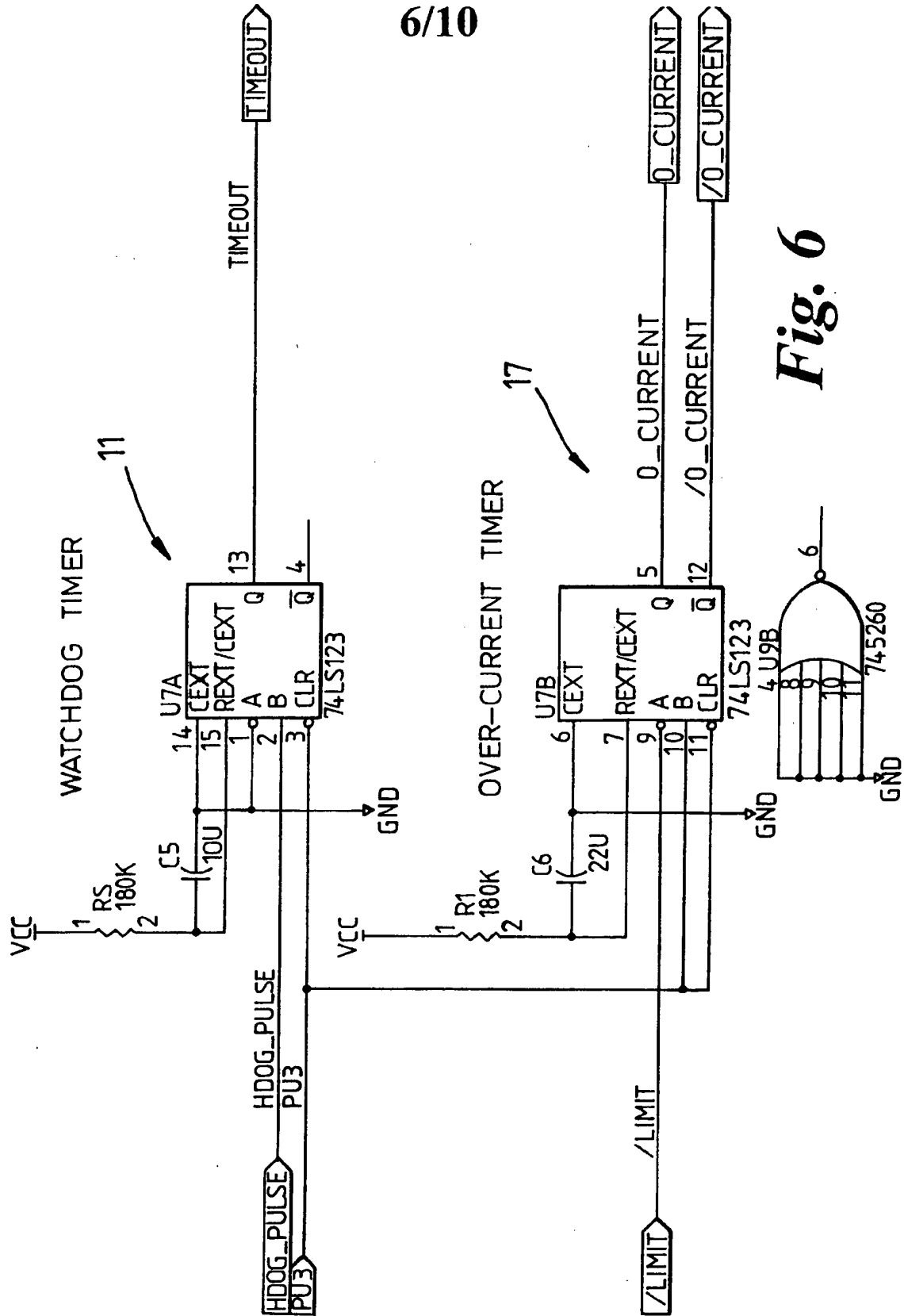


Fig. 6

7/10

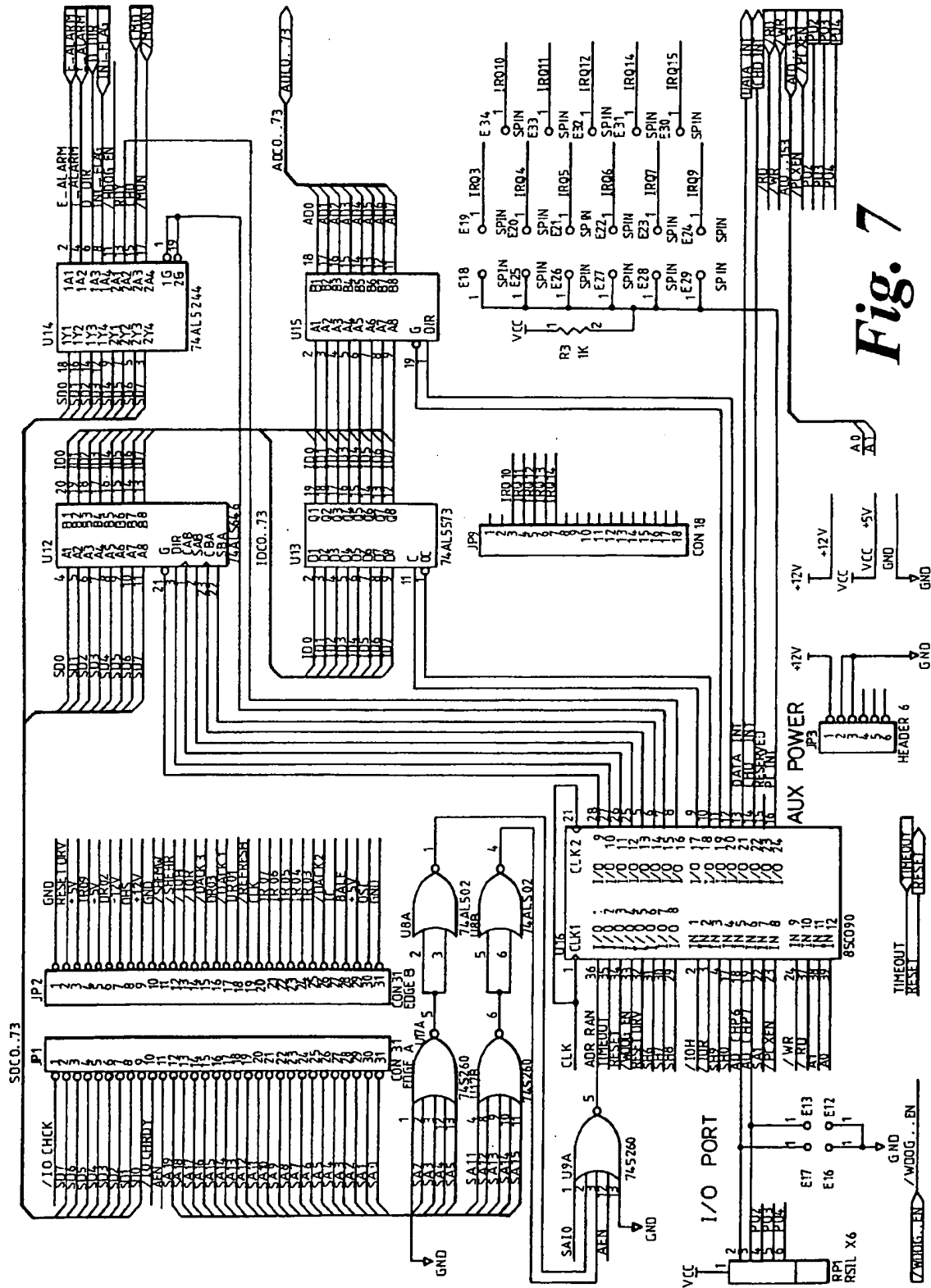


Fig. 7

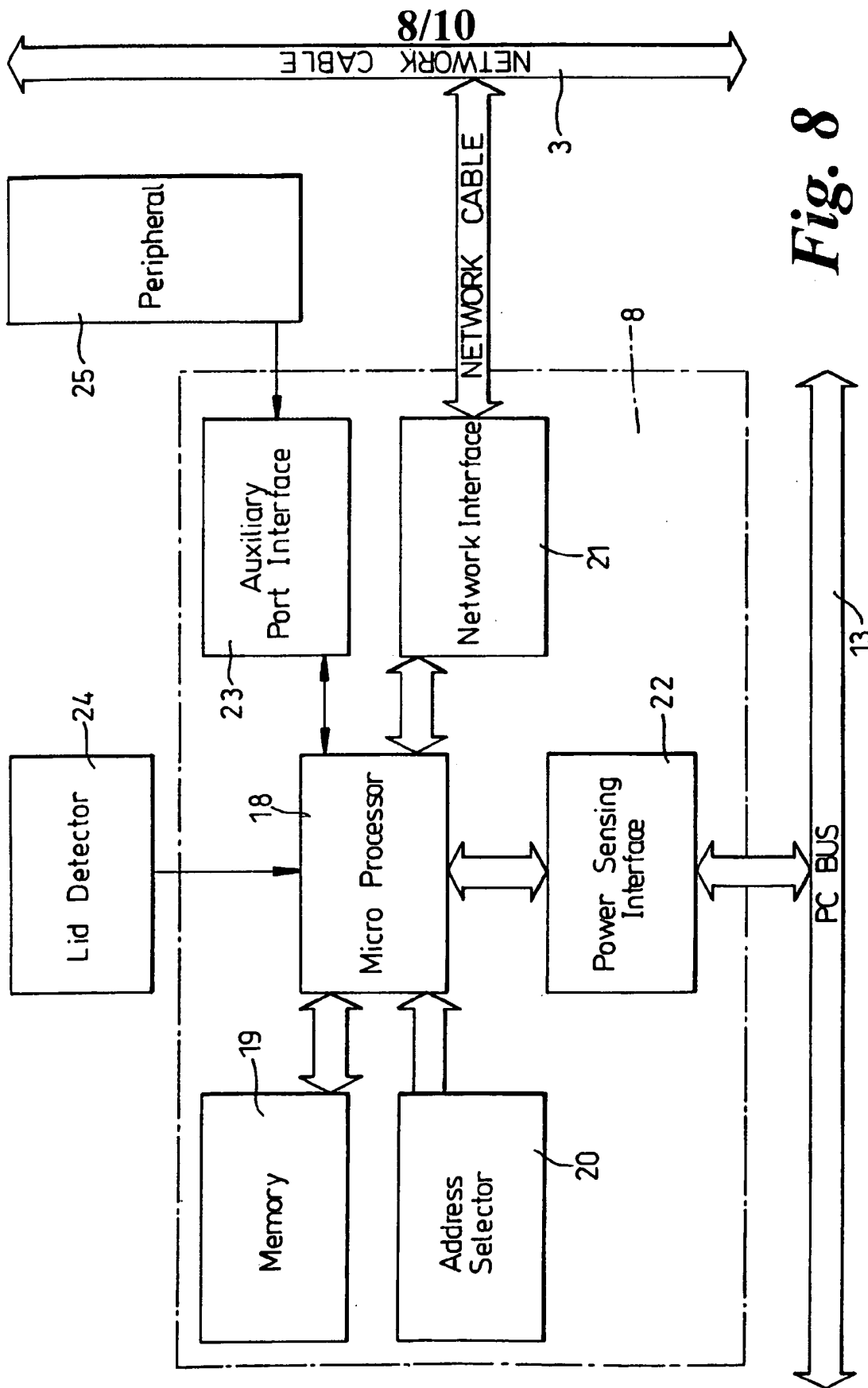


Fig. 8

9/10

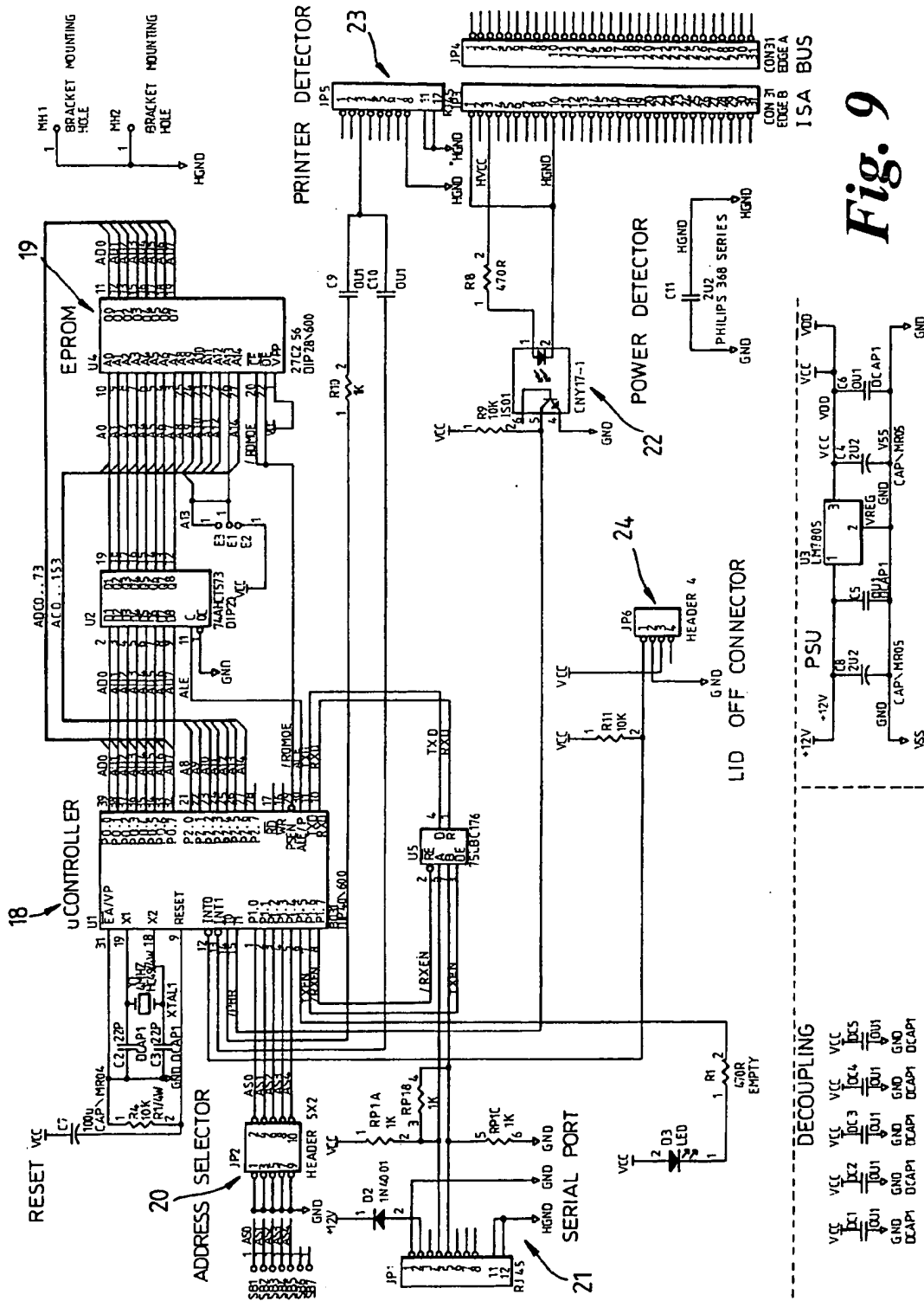
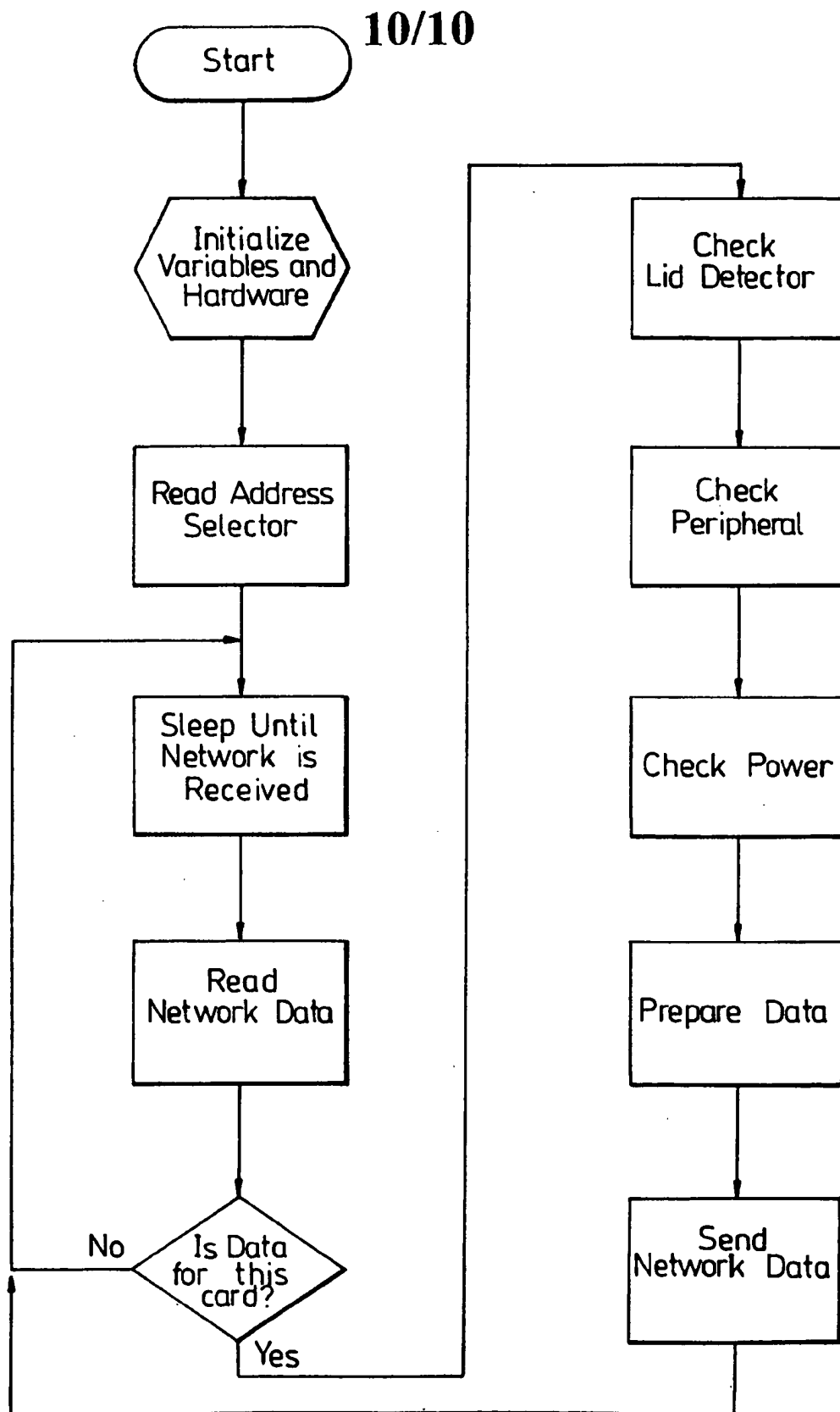


Fig. 9

**Fig. 10**

INTERNATIONAL SEARCH REPORT

Inter: 1st Application No

PCT/GB 97/03277

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G08B13/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 262 372 A (BACHE H. R. I.) 16 June 1993	1, 2
A	see the whole document	7
X	FR 2 719 689 A (CONTRACT OF SERVICES AND BUSINESS HOLDING OFFSHORE) 10 November 1995 see abstract	1, 2
A	US 5 268 668 A (BERUBE J. E.) 7 December 1993 see abstract	3
A	EP 0 734 005 A (BTICINO) 25 September 1996 see abstract	4
A	WO 94 17503 A (HONEYWELL) 4 August 1994 see claims 1, 2	5, 6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"G" document member of the same patent family

Date of the actual completion of the international search

2 March 1998

Date of mailing of the international search report

13/03/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sgura, S

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 97/03277

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2262372 A	16-06-93	AU 3089592 A CA 2125154 A EP 0615644 A WO 9311515 A	28-06-93 10-06-93 21-09-94 10-06-93
FR 2719689 A	10-11-95	NONE	
US 5268668 A	07-12-93	NONE	
EP 734005 A	25-09-96	IT MI950591 A	24-09-96
WO 9417503 A	04-08-94	US 5461372 A AU 673238 B AU 5995194 A CA 2147485 A CN 1094176 A DE 69403774 D DE 69403774 T EP 0680647 A ES 2102827 T JP 8506228 T	24-10-95 31-10-96 15-08-94 04-08-94 26-10-94 17-07-97 13-11-97 08-11-95 01-08-97 02-07-96

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.